State and Community Information Sharing and Analysis Organizations

Gregory B. White, Ph.D.
The University of Texas at San Antonio
Greg.White@utsa.edu

Keith B. Harrison, PhD
The University of Texas at San Antonio
Keith.Harison@utsa.edu

Abstract

For many years the importance of sharing information on cybersecurity risks, vulnerabilities, and incidents has been understood. Organizations working in isolation are at a disadvantage when facing the types of threats existing in today's Internet environment. Informal information sharing has been conducted for many years. More formal information sharing organizations were created in response to the 1998 Presidential Decision Directive-63. More recently, Executive Order 13691 called for the creation of information sharing and analysis organizations beyond the critical infrastructures and led to the creation of a standards organization to create standards, guidelines, and other documents to assist in the creation of information sharing organizations. This paper will discuss the history of information sharing in the United States and will explain the potential impact for states and communities. The importance of developing state and community information sharing organizations will be discussed along with the challenges in establishing them.

Keywords

Information Sharing, Computer Security, Computer Incident Response

1. Introduction

It is not hard to understand the benefit of information sharing and analysis in defending computer systems and networks. An attack discovered on one organization in a given sector might, and in fact most likely can, serve as a warning to others in the same sector. It is reasonable to assume that, for example, if an attack is occurring on a financial institution with a new vulnerability, it is very likely that others will be or already are also being attacked via the same vulnerability. If the first institution that detects the attack warns the other, many that might not have discovered the vulnerability until much later can address the problem at a much earlier point in time. It is also easy to imagine how sharing between sectors could also serve to provide similar early warning of attacks on an operating system or application that is used in multiple sectors. It might also provide an indication of an "inordinate interest" in an organization or geographic jurisdiction (such as a state or community) which might foreshadow a pending attack on the initial organization or upon others in the same sector or geographic region. Organizations that keep knowledge of attacks and unusual activity to themselves are actually doing a disservice to the security community at large.

The benefit in sharing of cybersecurity information has been recognized since the early days of the Internet. The earliest attempt to formalize a method to share cybersecurity information during a national incident occurred as a result of the Internet Worm released by Robert Morris. During the incident pockets of individuals around the country were attempting to address the incident and develop a defense for the worm. There were no established procedures or any formal method to share and coordinate information and efforts. After the event, meetings were held to discuss how best to handle similar situations in the future and in 1988 the Computer Emergency Response Team (CERT) at Carnegie Mellon University (CMU) was formed. The mission has evolved over time and many of the incident response functions now are part of the US-CERT located with the Department of Homeland Security (DHS) while the CERT/CC (CERT Coordination Center) housed at CMU now researches security vulnerabilities in software products and works with software vendors to develop methods to resolve discovered vulnerabilities. They also develop tools to assist organizations in conducting forensic examinations and in analyzing vulnerabilities. [1]

The next major advancement in cybersecurity information sharing organizations was the publication of Presidential Decision Directive/NSC-63 (PDD-63) in February, 1998. The subject of this PDD was broadly critical infrastructure protection. The stated intent of the PDD was to "assure the continuity and viability of critical infrastructures." [2] To do this, "the United States will take all necessary measures to swiftly eliminate any significant vulnerability to both

URI: http://hdl.handle.net/10125/41447
ISBN: 978-0-9981331-0-2

physical and cyber attacks on our critical infrastructures … especially our cyber systems." [2] Of importance to the discussion of information sharing, the PDD directed the FBI to expand its efforts to create a "national warning and information sharing system" and to "serve as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity." [2] It further encouraged the critical infrastructures to establish private sector sharing and analysis centers. These centers are now known as Information Sharing and Analysis Centers (ISACs). There are currently 24 member organizations in the National Council of ISACs (NCI) primarily covering the critical infrastructures.

Executive Order (EO) 13636, published in February, 2013, has the stated goal of improving the security and resilience of US critical infrastructure. To achieve this goal, the EO directs governmental agencies to partner with the owners and operators of critical infrastructure in order to "improve cybersecurity information sharing and collaboratively develop and implement risk-based standards." [3]

The first major contribution of EO 13636 is to increase the volume, timing, and quality of cybersecurity information sharing. To this end, DHS's Enhanced Cybersecurity Services (ECS) was expanded to include all 16 critical infrastructure sectors. ECS was also improved to provide near real time information sharing. Additionally, unclassified reports of threats to the US homeland are produced and disseminated in a timely manner to US private sector entities. Similarly, classified reports are made available to authorized critical infrastructure entities.

The second major contribution of EO 13696 was ordering the creation of a technology neutral and voluntary risk-based Cybersecurity Framework. The Cybersecurity Framework was developed by the National Institute of Standards and Technology (NIST) using voluntary consensus based standards. The objective of the framework is to provide standards, guidelines, and practices that are both cost-effective and applicable across all critical infrastructure sectors. [4]

Additionally, EO 13636 also contains provisions to protect privacy and civil liberties, establishes a program to promote and incentivize the adoption of cybersecurity practices, and orders the review of current cybersecurity regulatory requirements.

Presidential Policy Directive 21 (PPD-21), released at the same time as EO 13636, replaces HSPD-7 and dictates three strategic imperatives for the US Federal Government and critical infrastructure. First, PPD-21 refines the relationships between the US Federal Government, critical infrastructure, and State, Local, Tribal, and Territorial (SLTT) Governments, in order to facilitate better information sharing and collaboration. The second strategic imperative is the identification of requirements to enable the timely, efficient, and secure exchange of information between all levels of governments and critical infrastructure owners and operators. Finally, PPD-21 "calls for the implementation of an integration and analysis function for critical infrastructure that includes operation and strategic analysis on incidents, threats and emerging risks." [5]

The aforementioned Presidential Directives and Executive Order have been focused on information sharing between levels governments and critical infrastructure. However, one important piece of the information sharing puzzle has been left out, private sector cybersecurity information sharing. EO 13691 builds on EO 13636 and PPD-21 in order to address private sector cybersecurity information sharing by encouraging the development and formation of Information Sharing and Analysis Organizations (ISAOs). [6] EO 13691 specifies that ISAOs may be established as for-profit or nonprofit entities, and ISAO members may consist of private or public sector entities, or both. The Executive order calls for creation of ISAOs in order to promote cybersecurity information sharing within the private sector, between the private sector and the government, and between ISAOs.

EO 13691 instructs DHS to fund the creation of the "ISAO Standards Organization (SO), which shall identify a common set of voluntary standards or guidelines for the creation and functioning of ISAOs." [6] The standards developed by the ISAO SO are required to address the baseline services offered by ISAOs, and must, at a minimum address "contractual agreements, business processes, operating procedures, technical means, and privacy protections." [6]

Several provisions to protect privacy and civil liberties are present in EO 13691. The executive order specifically instructs the ISAO SO to include privacy protections, such as minimization, in the ISAO standards. Additionally, federal agencies engaged in activities under EO 13691 are directed to coordinate their activities "with their senior agency officials for privacy and civil liberties and ensure that appropriate protections for privacy and civil liberties are incorporated into such activities." [6]

Additionally, the ability of the government to engage in private-public cybersecurity information sharing between with ISAOs is improved by EO 13691. The National Cybersecurity and Communications Integration Center (NCCIC) is

directed to coordinate and collaborate with ISAOs on cybersecurity information sharing. The NCCIC is also designated as a critical infrastructure protection program and is given the authority to enter into voluntary agreements with ISAOs.

2. EO 13691 and the ISAO SO

As a result of EO 13691, DHS released a call for proposals to create the ISAO Standards Organization. A team from UTSA, LMI, and the Retail Cybersecurity Intelligence Sharing Center (R-CISC) was selected from the proposals submitted. Based on the details in the call for proposals and EO 13691, the ISAO SO has identified its mission as:

> *Improve the Nation's cybersecurity posture by identifying standards and guidelines for robust and effective information sharing and analysis related to cybersecurity risks/incidents and cybersecurity best practices.*

There are some foundational objectives that the ISAO SO established early. First, the documents produced must account for a wide range of potential ISAOs. A one-size-fits-all approach will not work for the robust ecosystem that it is envisioned for the ISAOs. The goal is to be as all-inclusive as possible so that any organization or individual that wants to participate in the cybersecurity information sharing program can do so.

A second principle is that the development of the documents is conducted in an open collaborative manner. Public comment will always be sought and anybody can participate in the public forums that are held periodically throughout the process. The actual documents are developed utilizing several working groups made up of volunteers interested in participating in the creation of the documents that emerging ISAOs will use. The entire process is conducted in a very public, open manner.

The third principle is one that has proven to be very critical. From the start, the standards and guidelines have been intended to be voluntary. There will not be a requirement for anybody to form or be part of an ISAO if they do not want to be part of one. As a result of interactions with government departments and the regulator community, some in industry have been concerned that participation in an ISAO may become mandatory within certain sectors. While the ISAO SO cannot prevent the federal government from creating laws that might move in this direction, the documents are currently being developed assuming a completely voluntary model. In fact, the ISAO SO sees part of its role as representing the views of the public and emerging ISAOs to various government agencies, ensuring that the public has an opportunity to provide input before laws or regulations are created in the information sharing space.

The final guiding principle is that documents that describe methods to conduct information sharing will take into account the need for confidentiality and privacy. Organizations who are members of an ISAO will want to ensure that any sensitive company information they share with that ISAO will remain confidential. Similarly, the privacy of individuals should be protected so that no personally identifiable information is released to individuals who do not have a need to view it.

It needs to also be pointed out that the ISAO SO recognized early in the process that, unlike other standard development organizations, standards will make up just one type of document that will be produced. EO 13691 states: "ISAO Standards Organization (SO), … shall identify a common set of voluntary standards or guidelines for the creation and functioning of ISAOs pointing out definitively that more than just standards are expected. In fact, it is believed that the ISAO SO will produce many more documents other than what is traditionally viewed as standards. These other documents may include discussions about what an ISAO is, how to form one, guidelines for what to consider in terms of services an ISAO may want to offer to its members, and templates for documents that may commonly be needed by an ISAO.

The ISAO SO formed six working groups to address various aspects of an ISAO and its creation. These working groups are made up of volunteers from government, academia, and industry and have been tasked with the actual creation of the documents that will be released by the ISAO SO. The six working groups are:

Working Group 1: ISAO Creation – This group was tasked with identifying and capturing the elements necessary for an interested organization to stand up an ISAO. These elements will serve as the basis for creating an ISAO and will have enough flexibility in design to fit the needs of diverse interested organizations.

Working Group 2: ISAO Services and Offerings – Since meeting the needs of its members will be critical aspect of all ISAOs, being able to determine what the needs are and what capabilities are needed to fulfill these needs is critical for all ISAOs. This working group will identify and capture

the capabilities necessary for an interested organization to effectively operate an ISAO. These services and offerings will support day-to-day operation of the ISAO and support its main function: to share and receive cyber information in a timely and effective manner. Capabilities must allow for the most basic ISAO and also support more sophisticated organizations. Not all ISAOs will provide the same capabilities and at least initially there is no definitive set of required capabilities for an entity to become and ISAO.

Working Group 3: Information Sharing – Obviously what needs to be shared and how will be a pressing issue that must quickly be addressed by each ISAO. This group will identify and capture items and develop the guidance necessary for an interested organization to effectively share cyber information (threat indicators, vulnerabilities, and best practices) within their ISAO or externally).

Working Group 4: Privacy and Security – There is a lot of concern over the issue of privacy (and confidentiality) and how information shared will remain secure and not released to individuals or organizations that are not authorized access to it. As a result, this working group was established to identify and capture the steps to safeguard information (both proprietary and privacy related). They will also detail the processes and procedures to prevent unauthorized release or access to information not cleared for release and will address how to meet Federal, State, Local, and Tribal laws regarding privacy.

Working Group 5: ISAO Support – This working group is quite a bit different from the others whose job is the creation of documents to be used by individuals and organizations forming an ISAO. It will consist of individuals familiar with the creation and operation of information sharing organizations who will work to support emerging ISAOs as they are created. This working group will work closely with the ISAO SO in providing this assistance to emerging ISAOs.

Working Group 6: Government Relations – While the ISAO SO is not a government entity (though its funding does come from DHS), the federal government will play a significant role in information sharing due to its intelligence gathering and analysis capability. This working group will identify and address issues associated with ISAO interactions with the Intelligence Community, Law Enforcement, US Regulators, and Homeland Security. It is expected that this communication will go both ways in that this working group will provide information to emerging ISAOs on what programs exist in the federal government for sharing of information with industry or the public but it will also provide feedback to the federal government on concerns expressed by the ISAOs related to government programs or capabilities.

Each of the groups have been asked to initially put together a draft of documents that will be needed for emerging ISAOs and that falls within the description of their working groups focus. These documents will be combined at their initial release to form what is in essence an ISAO Manual. The initial release of this document will not be complete but will provide what is immediately needed by emerging ISAOs with subsequent versions containing additional information.

3. The Information Sharing Ecosystem

As the ISAO SO develops the descriptions to allow for a wide range of ISAOs to be created, it becomes important to understand how the many different types will fit into what is being referred to as the Information Sharing Ecosystem. This is designed to explain the many different pieces that make up the ecosystem and how they all fit together into a unified information sharing program for the nation. The first part of the ecosystem are the different categories of ISAOs that may be formed. The initial capabilities document created by Working Group 2 identifies four major types of ISAOs which are:

Category 1: Individuals or Informal Group Based – This category would include: a self-employed security consultant; a localized group of professionals; and a group of security experts rapidly convened to address a new vulnerability of incident (in other words an issue-driven ISAO).

Category 2: Industry or Sector-based – This category would include the existing ISACs, and are what most individuals think of when ISAOs are mentioned. While some of the ISAOs created in Category 1 would be of limited duration, Category 2 ISAOs will be intended to be permanent (or at least for as long as they meet their members' needs).

Category 3: Geographically-based – ISAOs in this category will cross sector boundaries as they consist of all entities wishing to be members who are within a specific geographical boundary such as a city or state.

Category 4: Other – This category will consist of any ISAO that does not fit neatly into one of the other categories. It will include such entities as for-profit and not-for-profit ISAO service providers.

Since the creation of an ISAO is voluntary, it is easy to conceive that not all individuals or

organizations that are interested in sharing cybersecurity information will want to form or join an ISAO. The information sharing ecosystem needs to take into account this possibility and allow for a mechanism for all who want to participate in information sharing to be part of the national program.

A major player in the ecosystem will be several agencies within the federal government who are engaged in cybersecurity information sharing. In 2009, the NCCIC was created in order to analyze cybersecurity threats and vulnerabilities, share timely and actionable information with partners, and manage and support response and recovery efforts. The NCCIC partners with the private sector, critical infrastructure, SLTT governments, the US federal government, and international governments. The NCCIC is a central location that is currently comprised of four functional branches:

- **NO&I** - NCCIC Operations & Integration
- **US-CERT** - United States Computer Emergence Reediness Team
- **ICS-CERT** - Industrial Control Systems Cyber Emergency Response Team
- **NCC** - National Coordinating Center or Telecommunications

The premier cybersecurity information sharing program by DHS is called the Cyber Information Sharing and Collaboration Program (CISCP) and is part of the NCCIC. Joining the CISCP is free, and requires companies to sign a Cooperative Research and Development Agreement (CRADA). [7]

The flow of information in CISCP is bi-directional. Information shared with DHS is analyzed, aggregated, and anonymized and then shared with CISCP partners in the form of indicator bulletins, analysis reports, priority alerts, and recommended practices. Indicator bulletins are short and frequently issued announcements notifying partners of new threats that are intended to enable fast action. Analysis reports are an in depth analysis of a threat, including the activities of the adversary as well as methods for detecting and defending against the malicious activity. Priority alerts are intended to provide an early warning for specific significant threats. Recommended practices are the result of aggregating best practices received from CISCP partners.

Information is shared between CISCP partners using the Traffic Light Protocol (TLP). TLP helps to protect sensitive information by clearly defining what information may be shared with whom. [8] Information shared using TLP is assigned a specific color by the originator of the information:

- **RED** – The information is extremely sensitive and may not be shared with anyone outside of the specific exchange.
- **AMBER** – The information sensitive and should only be shared with members of the recipient's organizations that must have the information in order to act on it.
- **GREEN** – The information is useful and may be shared with any participants.
- **WHITE** – There is no or minimal risk of misuse and the information may be distributed to anyone.

A more recently created cybersecurity information sharing program provided by DHS and NCCIC is called Automated Indicator Sharing (AIS). Threat indicators that participants share with the NCCIC are shared anonymously with all participants without vetting by DHS in order to maintain faster, higher volume threat indicator sharing. DHS may, at their discretion, assign the information a reputation score if possible. In addition to participant developed indicators, DHS also develops and shares its own cyber threat indicators with AIS participants. [9]

AIS is free for private entities, US federal government, STTLT government, ISACs, ISAOs, as well as foreign governments and companies. Entities may participate in AIS by setting up the infrastructure necessary to connect directly to DHS, or by joining an ISAO or ISAC that participates in AIS. Information is shared among participants in AIS using Trusted Automated eXchange of Indicator Information (TAXII), Structured Threat Information eXpression (STIX), and CybOX.

TAXII is a set of specifications are used to define how and what cyber threat information is exchanged. These specifications are: TAXII overview, services specification, message binding specifications (e.g. XML), protocol binding specifications (e.g. HTTP), query format specifications, and content binding reference. It is up to each group using TAXII to decide what specifications best meets their needs. TAXII is designed to support sharing structured cybersecurity threat information such as STIX. [10]

STIX is a standardized language that makes use of CybOX in order to specify cybersecurity threat information. CybOX is a language for describing cyber observables. STIX is intended to capture the full range of possible cybersecurity threat elements including observables, indicators, incidents, tactics, techniques and procedures, exploit targets, courses of action, campaigns, and threat actors. [11]

4. Information Analysis

Most of the conversation about ISAOs has centered on the sharing of cybersecurity related information. This is an important and necessary first step but the real goal is to provide "actionable information" to the members of ISAOs. What is meant by this is that just sharing raw data or even facts about specific incidents does not immediately benefit a member of an ISAO. What members want is an analysis of all of the information gathered and a distillation of it down to a point that what they receive is information that they can take action on. They want to know what it is that they need to be doing as a result of the information that has been shared and not simply the large collection of shared information itself. This will be a major feature of the ISAOs and the real benefit that they will provide. It is also where the commercial entities that are forming to deliver ISAO services can play a critical role.

As in the information sharing aspect of an ISAO, the amount of analysis will vary between the ISAOs. While to be considered an ISAO some level of analysis needs to be accomplished, how detailed that analysis is will depend on the objectives of the individual ISAOs and on their services and offerings. For the more informal ISAOs the analysis could simply take the form of an email, teleconference, or simply a bulletin sent to all members. The important element is again that what is sent should be pertinent to the members of the ISAO and should discuss what the members should be doing as a result of the shared information and analysis.

At the other end of the spectrum, an advanced ISAO might conduct real-time analysis of ongoing events and shared information. The ISAO may employ 24x7 analysts and a Security Operations Center that monitors the status of the Internet as it relates to the ISAO members. This again is a place where potential ISAO service providers could greatly benefit their ISAO clients since it will be quite expensive to maintain a 24x7 operation center with security analysts.

While an ISAO service provider with its own security analysts will have the ability to determine what information is critical for the members of an ISAO, the various federal agencies involved in information sharing and analysis have access to information that the commercial entities will often not have. Though some of the service providers may argue the opposite is also true, it is hard to argue with the fact that the various intelligence gathering agencies of the federal government have resources that most commercial entities do not have access to. Sharing of information with the organizations the federal government has set up to participate in information sharing efforts can provide a level of analysis and access to information that otherwise may not be possible. ISAOs should therefore seriously consider participating with the programs to share more detailed and analyzed information established by these federal agencies. In order to participate, ISAOs will generally be required to agree to a certain level of vetting by the federal agency.

For some, submitting to the vetting of their organization or their members is not something that they want to do. Indeed, there are many who may not want to share any of their information with a government entity at all. Whether this is done or not is up to the individual ISAOs and their members and the decision to do so is completely voluntary – there is no requirement to share with the federal government if the ISAO and its members do not wish to share. The hesitation to share, not only with the federal agencies but with other ISAOs or even between members of a specific ISAO is often centered around the desire to ensure privacy and confidentiality of information. This is one of the challenges facing emerging ISAOs.

5. Challenges Facing the ISAOs

There are a number of challenges facing organizations and individuals wishing to form an ISAO and that face the entire information sharing ecosystem itself. Among these challenges are privacy and confidentiality, trust, scalability, certification of ISAOs, the willingness to share information, and the funding of ISAOs. An emerging ISAO will have to address each of these issues.

Concerns around privacy and confidentiality of information shared is a major concern to organizations wanting to participate in an ISAO. They want to be assured that any information that an organization shares with others, no matter who those others are (i.e. other members, other ISAOs, and/or federal agencies involved in information sharing programs), will be kept private and confidential and only released to individuals or organizations that have a right to have access based on the agreements that are signed by members of an ISAO. For purposes of this discussion, the difference between privacy and confidentiality is that privacy is generally used in the context of information sharing to mean personal information about individuals within a member organization should remain private. Confidentiality refers to information about the organizations – information that might give others a competitive advantage should the information become public or known to a competitor. How sensitive this issue is can be seen in the debate that

surrounded the passing of the Cybersecurity Information Sharing Act (CISA) in the United States in 2015. The act was ultimately passed but there was some significant opposition to it based on the belief that compliance with the act would provide the federal government access to personal information they would otherwise not have had access to. Subsequent clarification of the provisions of the act have shown that these concerns were not justified as the act provided clear guidance on the "scrubbing" of personal information before any information was shared with the government. Nonetheless, the debate that surrounded the passing of the act provides an indication of just how sensitive of a subject this is.

Trust is another issue that will have to be addressed by all parties involved in the information sharing ecosystem. The concern is what level of trust can be placed in the information that has been received from another part of the ecosystem. How reliable is the information that has been shared? Do the individuals that have provided the information have a level of expertise to truly understand what they have reported or is the information they provided an incorrect understanding of a specific situation? Is it possible for deliberately false or misleading information to be inserted into the ecosystem? If organizations within an ISAO do not need to be vetted, then is there the possibility that an ISAO will be formed by individuals hostile to the information sharing ecosystem and that may then inject false or misleading information which could impact the actions of others? While the fact that these issues are something that needs to be addressed is well understood, currently the ISAO SO and its working groups have not developed any guidance on how trust will be handled. Currently information shared between ISAOs and federal agencies that have vetted them are considered to be reliable, as well as information shared between ISAOs that have established a relationship of trust. Further trust is left up to the ISAOs themselves though guidance on this will be forthcoming.

Some have suggested that a vetting process or certification of the ISAOs would handle issues of trust and would provide a level of confidence that procedures to protect privacy and confidentiality of information are in place. While this may be true, the original guidance provided to the ISAO SO is that ISAOs should be able to self-certify. This obviously impacts the level of trust that can initially be placed in any given ISAO. The guidance from the ISAO SO will allow for self-certification but also being examined is whether another level of certification would be beneficial to the program and if so, how will this certification process be conducted?

Scalability is an issue that can be immediately seen when discussing the possibility of 100's or 1000's of ISAOs emerging. Add to this the fact that any given individual or organization could potentially be a member of multiple ISAOs and the possibility of an overwhelming amount of information being entered into the ecosystem becomes a real issue. An overwhelming amount of information will do nothing to enhance the security of the nation but could in fact have a negative impact on its overall current security status. Initially the ISAO SO is suggesting that this issue be addressed at the individual ISAO level. In other words, member organizations should not be the ones that have to face an overwhelming amount of information but rather the ISAOs themselves. The members should always only be receiving actionable information from the ISAO they are a member of. How the ISAOs will handle the potential for too much information is an issue that is being addressed by the ISAO SO but for which there is no current guidance.

Probably the most basic of issues that the ISAOs have to overcome is an understanding of why it is important to share information. For those who have been heavily involved in cybersecurity for years this is not as much of an issue, the value of sharing is fairly clearly understood. Those who do not have an understanding of the importance, however, need to be convinced that sharing information about security indicators and incidents will ultimately be beneficial. If for no other reason than today it may be one organization that gets hit, tomorrow it may be a different organization that first discovers an ongoing breach. If everybody shares, then today one organization may be the beneficiary of such sharing while tomorrow it may be somebody else. The other important thing to emphasize is that sharing of information does not mean a wholesale sharing of all information about the security status of a company. Reports can, and should, be sanitized to highlight the necessary items and not provide confidential information about a company or its security controls.

The final issue to mention here is a less technical one but one that will be critical for emerging ISAOs. This is the funding of ISAOs. The ISACs generally charge a membership fee for an organization to receive information for that sector. Organizations within that sector can determine whether there is a sufficient value proposition for them to pay that membership fee. The much more all-inclusive nature of ISAOs will lead to less formal ISAOs which may not charge a membership fee. The fee provides for the funding of full-time analysts and support personnel. If this level of support is not needed based on the objectives of a specific ISAO, then funding

may not be needed and a membership fee may not be required. On the other hand for members that want more real-time intensive analysis and actionable information, the more full-time staff or paid services will be required. This may impact the services and offerings that an ISAO develops as some ISAOs whose membership includes a majority of small businesses may not be able to charge fees sufficient to support more extensive analysis services. This will be up to the individual ISAOs to determine.

6. Current Status

Since the selection of the team to implement the ISAO SO in October 2015 a lot has been accomplished. Two major tasks faced the SO at the outset: 1) to analyze the work that had already occurred in the ISACs that have been in operation for more than a decade and the multiple meetings that were held on the subject of information sharing and analysis before the selection of the SO; and 2) to establish the working groups that would be the 'workhorse' for the SO and would be the entities that would actually develop the standards, guidelines, and other documents. The SO got a quick start by holding the first of four open, public forums within 45 days of when the grant was awarded. This initial meeting, held in Tysons, VA, brought individuals interested in cybersecurity information sharing together to discuss what had already occurred in the space and to begin to identify the working groups that would be formed.

The next public forum was held in San Antonio, TX, and the most significant part of this meeting was the opportunity for the recently established six working groups to meet and discuss their way ahead. Following this meeting the working groups began the real work on the first draft documents which were released for public comment before the 3rd public forum which was held in Anaheim, CA in May. Between this 3rd meeting and the 4th meeting, held back in Tysons, VA in August, the second call for public comments on the draft documents occurred. The working groups then considered each of the public comments received and created the final version of the initial documents which was released in September, 2016.

The initial draft documents (which were developed individually by the different working groups but which were then combined into a unified document for the September release) consisted of the following:

1. The ISAO categories and capabilities
2. A model for ISAO interaction
3. Information collection and dissemination
4. An examination of ISAO security and privacy issues
5. An examination of federal government programs and services related to information sharing and analysis

In addition to these documents, a support and mentoring infrastructure and process was put into place to assist emerging ISAOs to establish themselves.

The initial set of capabilities was not considered to be a definitive list. What it conveyed were thoughts about what capabilities an ISAO might want to consider when being established. Further services and services and offerings will be added as they are identified which may occur in the next year or may be added when new technology or approaches are developed well into the future. The ISAO program is an ongoing effort without a programmed end date.

Even before the release of the initial document(s), the ISAO SO began to receive requests by individuals and organizations to establish new ISAOs. An outreach and stakeholder engagement program along with a support function and mentorship program, were established to work with these new entities and to publicize the SO and to advertise the method under which new ISAOs could be created. At this point, the formation of ISAOs is moving forward along with the establishment of the conceptual information sharing ecosystem. As expansion continues, work will be accomplished to address the issues previously mentioned as they arise.

7. Future Timeline and Work

While much has been accomplished in the year since the creation of the ISAO SO, much still needs to be accomplished. The challenges previously mentioned needs considerable work to establish the information sharing ecosystem that all may participate in. The scalability issue and what information needs to be shared are tied together since ISAOs want to share only the minimum amount of information in order to be able to provide the actionable information their members' desire. This is the major issue that needs further work in the future – devising a plan for sharing information across all categories of ISAOs across the entire ecosystem will be a considerable challenge in the future.

Another goal in the future is the expansion of the number of ISAOs and an expansion of the membership in existing ISAOs. Ultimately we want

everybody to be part of the ecosystem at some level. Their choice will be at what level they will want to participate in sharing of information.

The current ISAO effort within the United States has sidestepped the issue of the international nature of cybersecurity. Participation of multi-national corporations in information sharing is understood. This is already occurring. What has not been addressed by the ISAO SO and its working groups is an examination of the laws and requirements in different countries for privacy, confidentiality, and the reporting of incidents. Instead, the way the current documents have been developed is to emphasize those issues that are considered core information sharing and analysis leaving country-specific items to appendices which can be added as additional countries examine the core principles and how they relate to each additional country or region. The focus thus has been on aspects of information sharing and analysis that is common across international boundaries.

Finally, the initial grant called for a 5-year effort but it was quickly realized that for the ISAOs to survive beyond the 5-year point some long-term structure needs to be developed with consistent funding to ensure that future technology that may impact the current thought on information sharing and analysis along with changes to laws that might impact certain countries would need to be incorporated into the guidance that had been produced. Who will be responsible for the long-term sustainment of the ISAO effort?

8. Conclusion

The benefit of cybersecurity information sharing to prevention, detection, response, and recovery to cybersecurity incidents has been adequately shown through the decade-long effort of the current ISACs. ISACs alone, however, do not cover the entire landscape of organizations within the country that need to be participating in information sharing. This has prompted the development of a standards organization to address standards and guidelines that emerging ISAOs will need to incorporate. The ISAO SO is this organization and it is utilizing working groups in an open, collaborative, and very public program to develop the documents needed. This is an on-going effort though the initial set of documents has been created. Much still remains to be accomplished, and the working groups continue to expand on the documents that have already been developed.

The process being utilized is an open, public, collaborative effort and anybody who wishes to be part of the effort may volunteer to be on one of the working groups, attend one of the open forum meetings that are held to provide a forum for the public to raise concerns or questions about what is being developed, or through the online comment process that allows anybody to provide feedback on the documents that have been developed – especially during the draft comment phase of the effort. More information can be found at www.ISAO.org.

9. References

[1] CERT Coordination Center, "About Us", www.cert.org/about .

[2] PDD-63, http://fas.org/irp/offdocs/pdd/pdd-63.htm

[3] Exec. Order No. 13636, 3 C.F.R., 2013.

[4] National Institute of Standards and Technology, "Framework for improving critical infrastructure cybersecurity", February 12, 2014.

[5] The White House, "Presidential policy directive 21: critical infrastructure security and resilience (ppd-21)," Feb. 12, 2013.

[6] Exec. Order No. 13691, 3 C.F.R., 2015.

[7] "Cyber information sharing and collaboration program (ciscp)," https://www.dhs.gov/ciscp, May 2016

[8] "Traffic light protocol (tlp) matrix and frequently asked questions," https://www.us-cert.gov/tlp, July 2016.

[9] "Automated indicator sharing (ais)," https://www.us-cert.gov/ais, July 2016.

[10] Julie Connolly, Mark Davidosn, and Charles Schmidt, "The trusted automated exchange of indicator information (taxii)," Retrieved from http://taxii.mitre.org/about /documents/Introduction_to_TAXII_White_Paper_May_2014.pdf, February 2014.

[11] Sean Barnum, "Standardizing cyber threat intelligence information with the structured threat information expression (stix)," Retrieved from http://stix.mitre.org/ about/documents/STIX_Whitepaper_v1.1.pdf, Connolly, May 2014.

The ISAO SO effort is supported by a grant through the Department of Homeland Security.